UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/803,788 | 03/17/2004 | Hristo Iankov Bojinov | 112056-0474 | 8050 |

24267 7590 01/05/2010

CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

| EXAMINER | |
|---|---|
| COLAN, GIOVANNA B | |
| ART UNIT | PAPER NUMBER |
| 2162 | |
| MAIL DATE | DELIVERY MODE |
| 01/05/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/803,788 | BOJINOV ET AL. | |
| | Examiner | Art Unit | |
| | GIOVANNA COLAN | 2162 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5 and 30-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 30-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is issued in response to the Amendment filed on 09/08/2009.

2. Claims 1 – 2, 30 – 35, 38, and 40 – 44 were amended. Claims 6 – 29 were canceled. No claims were added.

3. This action is made Final.

4. Claims 1 –5, and 30 – 67 are pending in this application.

### *Response to Arguments*

5. Applicant's arguments filed 09/08/2009 have been fully considered but they are not persuasive.

### *Claim Rejections - 35 USC § 103*

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 –5, and 30 – 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chandrashekhar et al. (Chandrashekhar hereinafter) (2005/0033988 A1) in view of Ryuutou et al. (Ryuutou hereinafter) (US 2002/0083191).

Regarding Claim 1, Chandrashekhar discloses a method for establishing identity in a file system, comprising:

Receiving, from a client, a first Network File System (NFS) operation ([0037], "NFS", Chandrashekhar) concerning an indicated file, the first NFS operation received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first NFS operation from the proxy to be received by a file server (Page 4, [0062] - [0065], Chandrashekhar);

returning a NFS file handle associated with the first NFS operation ([0037], "NFS", Chandrashekhar) from the file server to the proxy in response to the file server receiving the first NFS operation from the proxy (Page 4, [0066], Chandrashekhar);

inserting, by the proxy, metadata into the NFS file handle in response to receiving the NFS file handle from the file server ([0037], "NFS", Page 3 and 4, [0055], "The directed proxy server is adapted to provide policy information on either or both the header information and the trailer information...", and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar), wherein the metadata is an encryption key ([0055], lines 6 – 9, Chandrashekhar).

Chandrashekhar also discloses sending, by the proxy in response to receiving the NFS file handle from the file server ([0037], "NFS", Chandrashekhar), the NFS file handle to the client as a reply to the first NFS operation (Page 4, [0070] and [0037], Chandrashekhar). However, Chandrashekhar does not explicitly disclose sending, by the proxy the file handle with the metadata inserted in the file handle to the client. On the other hand, Ryuutou discloses: inserting, by the proxy, metadata into the file handle

in response to receiving the file handle from the file server ([0072], and [0073], Ryuutou); and sending, by the proxy in response to receiving the file handle from the file server, the file handle with the metadata inserted in the file handle to the client as a reply to the first NFS operation; and using the metadata and the file handle in a second operation to identify the client and the indicated file ([0074], Ryuutou). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chandrashekhar by incorporating the step of sending, by the proxy, the file handle with the metadata inserted, in the same conventional manner as disclosed by Ryuutou. Skilled artisan would have found it motivated to use such a modification in order to improve the response performance of a CORBA communication using the HTTP tunneling by making a communication corresponding to a communication connection request from a client within one session via the same different Web server, in view of the above described problem (see; [0016], Ryuutou).

With respect to claims 32, and 38, the claims are rejected under the same grounds as claim 1.

Regarding Claims 2, 34, 47, and 60, the combination of Chandrashekhar in view of Ryuutou discloses a method, whereby:

using the metadata in the NFS file handles eliminates a need for the proxy to generate additional requests to the file server to establish file identity, and for

completing client requests ([0037], "NFS", Page 4, [0085], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou).

Regarding Claims 4, and 36, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

using an NFS file system as the file system (Page 3, [0037], Chandrashekhar).

Regarding Claims 5, and 37, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

using a stateless protocol by the file system (Page 3, [0037], Chandrashekhar).

Regarding Claims 30, and 33, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

receiving, from the client, a second NFS operation by the proxy ([0037], "NFS", Page 4, [0061], Chandrashekhar), the second NFS operation comprising the metadata in a further NFS file handle sent with the second request ([0037], "NFS", Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], Ryuutou);

identifying, in response to the metadata, the client as to submit the second NFS operation ([0037], Page 4, [0068], Chandrashekhar);

sending the second NFS operation to the file server and not sending the metadata with the second NFS file handle to the file server ([0037], Page 4, [0070],

Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

receiving by the proxy a further NFS reply from the file server, and sending by the proxy the further NFS reply to the client ([0037], Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claim 31, the combination of Chandrashekhar in view of Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

returning a reply associated with the first file request from the file server to the proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle associated with the indicated file (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, metadata into the file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar);

sending, by the proxy, the file handle with the metadata inserted in the file handle to the client, the metadata to be used in further requests to identify the client as having

a permission to access the indicated file ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

receiving, from the client, a second file request by the proxy (Page 4, [0061], Chandrashekhar), the second file request including the metadata in a further file handle sent with the second request (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

identifying, in response to the metadata, that the client has the permission to submit the second file request ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

sending the second file request to the file server and not sending the metadata with the second file handle to the file server (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou); and

receiving by the proxy a second reply from the file server, and sending by the proxy the second reply to the client (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou).

Regarding Claims 39, and 45, the combination of Chandrashekhar in view of Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

granting permission for the request to be acted upon by the file system in response to a predetermined protocol ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

returning a reply associated with the first file request from the file server to the proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle associated with the indicated file (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, a session key into the file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar; and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

sending, by the proxy, the file handle with the session key inserted in the file handle to the client, the session key to be used in further requests to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claims 40, and 46, the combination of Chandrashekhar in view of Ryuutou discloses a non-volatile memory, further comprising:

receiving, from the client, a second NFS operation by the proxy ([0037], Page 4, [0061], Chandrashekhar), the second NFS operation comprising a session key in a second NFS file handle sent with the second NFS operation ([0037], [0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou);

identifying, in response to the session key, that the client has the permission to submit the second NFS operation ([0037], [0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

sending the second NFS operation to the file server and not sending the session key with the second NFS file handle to the file server ([0037], Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

receiving by the proxy a second NFS reply from the file server, and sending by the proxy the second NFS reply to the client ([0037], Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claims 43, and 49, the combination of Chandrashekhar in view of Ryuutou discloses a non-volatile memory, further comprising:

using a NFS file server as the file server (Page 3, [0037], "NFS", Chandrashekhar).

Regarding Claims 44, and 50, the combination of Chandrashekhar in view of Ryuutou discloses a non-volatile memory, further comprising:

using a two way communication exchange between the proxy and the file server (Fig. 1, Chandrashekhar).

Regarding Claim 51, the combination of Chandrashekhar in view of Ryuutou discloses an apparatus to establish identity in a file system, comprising:

a proxy configured to receive a first file request sent by a client to a file system, the proxy further configured to forward the first file request to a file server (Page 4, [0059] - [0061], Chandrashekhar);

the file server configured to return a reply associated with the first file request to the proxy (Page 4, [0066], Chandrashekhar);

the proxy further configured to insert a session key into a file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar);

the proxy further configured to send the file handle with the session key inserted in the file handle to the client, the session key configured to be used in a second file

request to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

the proxy further configured to receive, by the client, a second file request (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar), the second file request configured to include the session key in a second file handle sent with the second file request ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

the proxy further configured to receive the second file request, and the proxy to identify, in response to the session key, the client having a permission to submit the second file request, and the proxy to send the second file request to the file server and not to send the session key with the second file handle to the file server ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou); and

the proxy further configured to receive a second reply from the file server, and the proxy further configured to send the second reply to the client (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou).

Regarding Claims 52, and 58, the combination of Chandrashekhar in view of Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a first file request concerning an indicated file from a client, the first file request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the first file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

determining that the client has a permission to have the request acted upon by the file system in response to a predetermined protocol ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

returning a reply associated with the first file request from the file server to the proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle associated with the indicated file (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, a cryptographic information into the file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar; and also see Page 4, [0077] and [0078], Chandrashekhar);

sending, by the proxy, the file handle with the cryptographic information inserted in the file handle to the client, the cryptographic information to be used in one or more requests to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claims 53, and 59, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

receiving, by the client, a second file request by the proxy, the second file request including the cryptographic information in a second file handle sent with the second file request (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

identifying, in response to the cryptographic information, that the client has permission to submit the second file request ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0068], Chandrashekhar);

sending the second file request to the file server and not sending the cryptographic information with the second file handle to the file server (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou); and

receiving by the proxy a second reply from the file server, and sending by the proxy the second reply to the client (Page 4, [0070], Chandrashekhar).

Regarding Claims 56, and 62, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

using a NFS protocol as the predetermined protocol (Page 3, [0037], Chandrashekhar).

Regarding Claims 57, and 63, the combination of Chandrashekhar in view of Ryuutou discloses a method according, further comprising:

using as the predetermined protocol a two way communication exchange between the proxy and the file server (Fig. 1, Chandrashekhar).

Regarding Claim 64, the combination of Chandrashekhar in view of Ryuutou discloses an apparatus to establish identity in a file system, comprising:

a proxy configured to receive a first file request sent by a client to the file system, the proxy to forward the first file request to a file server (Page 4, [0059] - [0061], Chandrashekhar);

the file server configured to return a reply associated with the first file request to the proxy (Page 4, [0066], Chandrashekhar);

the proxy further configured to insert a cryptographic information into a file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar);

the proxy further configured to send the file handle with the cryptographic information inserted in the file handle to the client, the cryptographic information configured to be used in a second file request to identify the client and the indicated file (Page 4, [0070], Chandrashekhar);

the proxy further configured to receive, by the client, a second file request, the second file request configured to include the cryptographic information in a second file handle sent with the second file request (Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou);

the proxy further configured to identify the second file request, in response to the cryptographic information, the client as having a permission to submit the second file request (Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou); and

the proxy further configured to send the second file request to the file server and not to send the cryptographic information with the second file handle to the file server ([0009], "The method includes requesting for a file from a client to the proxy server and authenticating a requesting user of the client", Page 4, [0085] and [0059], Chandrashekhar; and [0072], [0073], [0074], "...subsequent communication connection requests...", Ryuutou); and

the proxy further configured to receive a second reply from the file server, and the proxy to send the second reply to the client (Page 4, [0070], Chandrashekhar).

Regarding Claim 65, the combination of Chandrashekhar in view of Ryuutou discloses a method for establishing identity in a file system, comprising:

receiving a file request concerning an indicated file from a client, the request received by a proxy (Page 4, [0059] - [0061], Chandrashekhar);

forwarding the request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

returning a reply associated with the file request from the file server to the proxy (Page 4, [0066], Chandrashekhar), wherein the reply includes a filed handle associated with the indicated file (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

inserting, by the proxy, metadata into the file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], Ryuutou); and

sending, by the proxy, the file handle with the metadata inserted in the file handle to the client, a size of the file handle set to a sum of a length of the server file handle and a length of the proxy metadata ([0012], and [0038], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou), the metadata to be used in further requests to identify the client and the indicated file (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claim 67, and 66, the combination of Chandrashekhar in view of Ryuutou discloses a computer apparatus, comprising:

a proxy configured to receive a client file request for a file (Page 4, [0059] - [0061], Chandrashekhar) and forward the file request from the proxy to a file server (Page 4, [0062] - [0065], Chandrashekhar);

the server configured to return a reply associated with the file request (Page 4, [0066], Chandrashekhar), wherein the reply includes a file handle (Figure 7, item: "Receiving file data from NAS server", Chandrashekhar; and Page 3, [0053], Ryuutou);

the proxy further configured to intercept the file handle sent from the server and insert metadata into the file handle to create a modified file handle (Page 3 and 4, [0055] and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], [0073], Ryuutou);

the proxy further configured to send the modified file handle with the metadata inserted in the file handle to the client ([0012], and [0038], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou); and

the proxy further configured to receive the modified file handle from the client for a second file request for the file, wherein the proxy is further configured to use the modified file handle to eliminate a need for the proxy to generate one or more additional requests to the server that would be required to access the file if the modified file handle did not include the inserted metadata (Page 4, [0070], Chandrashekhar; and [0072], [0073], [0074], "…subsequent communication connection requests…", Ryuutou).

Regarding Claims 3, and 35, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

encoding metadata in a form of a session key into the file handle, the session key expiring after a predetermined amount of time ([0057 – [0059], Ryuutou).

Regarding Claims 41, and 48, the combination of Chandrashekhar in view of Ryuutou discloses a non-volatile memory according to claim 39, further comprising:

causing the session key to expire after a selected amount of time ([0057 – [0059], Ryuutou).

Regarding Claim 42, the combination of Chandrashekhar in view of Ryuutou discloses a non-volatile memory, further comprising:

causing the session key to expire after a selected amount of usage ([0057 – [0059], Ryuutou).

Regarding Claims 54, and 61, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

causing the cryptographic information to expire after a selected amount of time ([0057 – [0059], Ryuutou).

Regarding Claim 55, the combination of Chandrashekhar in view of Ryuutou discloses a method, further comprising:

causing the cryptographic information to expire after a selected amount of usage ([0057 – [0059], Ryuutou).

***Response to Arguments***

8. Applicant argues that the applied art fails to disclose: "inserting, by the proxy, metadata into the NFS file handle, wherein the metadata is an encryption key; and sending the NFS file handle with the metadata inserted in the NFS file handle to the client as a reply to the first NFS operation".

Examiner respectfully disagrees. the combination of Chandrashekhar in view of Ryuutou does disclose: inserting, by the proxy, metadata into the NFS file handle (Page 3 and 4, [0055], "The directed proxy server is adapted to provide policy information on either or both the header information and the trailer information...", and [0067] – [0069]; respectively, Chandrashekhar and also see Page 4, [0077] and [0078], Chandrashekhar; and [0072], and [0073], Ryuutou), wherein the metadata is an encryption key ([0055], lines 6 – 9, Chandrashekhar); and sending the NFS file handle with the metadata inserted in the NFS file handle to the client as a reply to the first NFS operation ([0074], Ryuutou). See also rejection of claims 1, 32, and 38 discussed in this Office Action above.

***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to GIOVANNA COLAN whose telephone number is (571)272-2752. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Giovanna Colan
Examiner
Art Unit 2162
December 28, 2009

/John Breene/
Supervisory Patent Examiner, Art Unit 2162